

TeleTrust-EBCA "PKI-Workshop" 2023

Berlin, 21.09.2023

"eIDAS Novellierung: Status Qualifizierte Zertifikate für Websiteauthentifizierung (QWAC)"

Christian Seegebarth, D-Trust GmbH

Die Vertrauensdienste der eIDAS-Verordnung* sorgen für Sicherheit und Transparenz in der digitalen Welt



Elektronische Signatur

Die individuelle digitale Unterschrift



Elektronisches Siegel

Der verlässliche digitale Stempel für Behörden und Unternehmen



Website-Zertifikat (QWAC)

Die sichere Identifizierung eines Website-Betreibers oder einer Relying Party



Validierungsdienst

Der automatische unabhängige Prüfer



Einschreib- und Zustelldienst

Die sichere digitale Nachricht wie bei der Post oder dem Gerichtsvollzieher



Zeitstempel

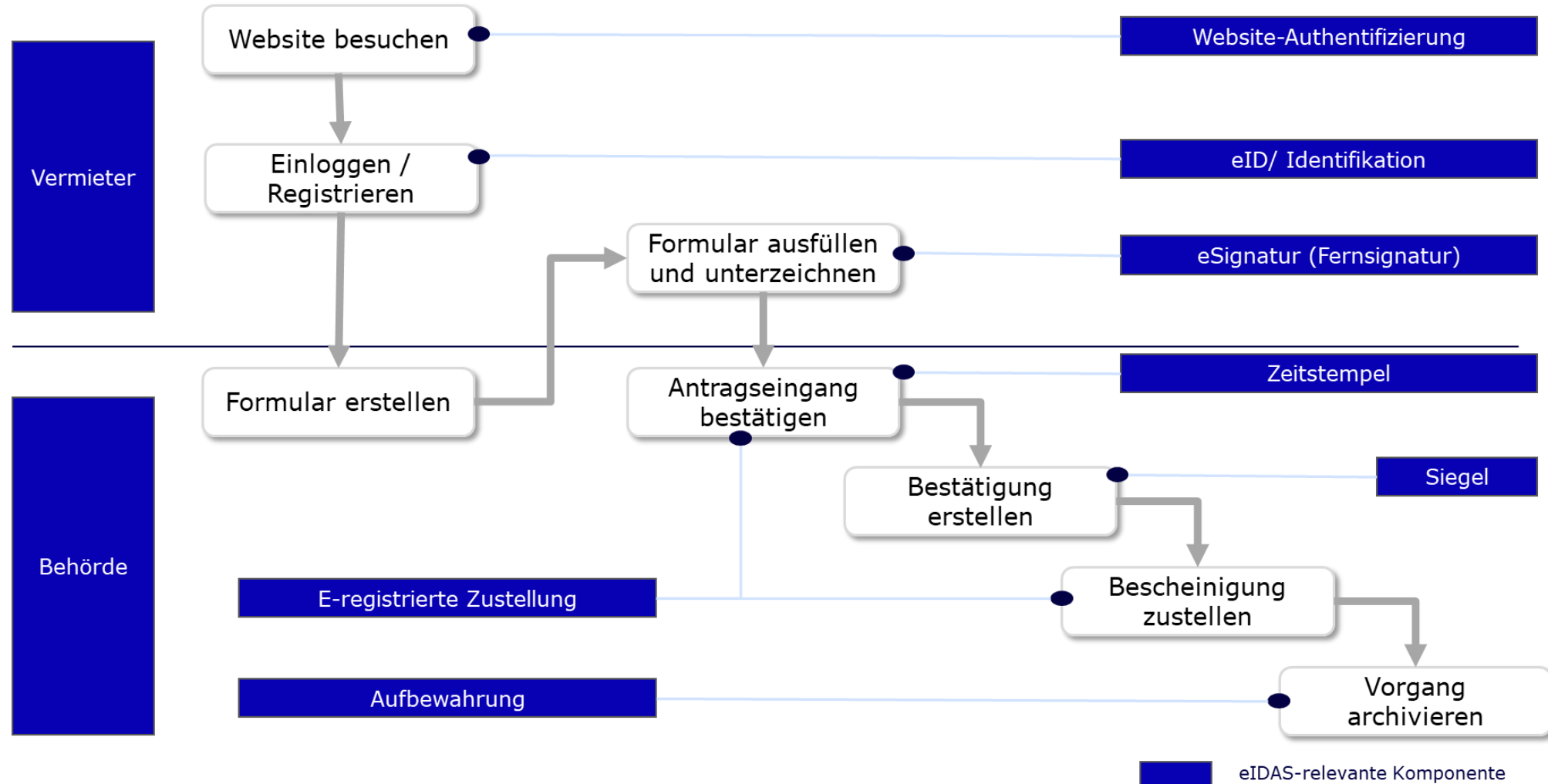
Die offizielle Zeit wie ein elektronischer Fotobeweis



Bewahrungsdienst

Beweiswerterhaltung

eIDAS - Vertrauensraum



„The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020“.

The eID has failed.

Trust services are
successful.

No potential of
further development
in the public sector.

Poor private sector
connectivity to notified
systems.

Struktur der neuen eIDAS Verordnung

Current structure

Chapter I – General provisions

Chapter II – Electronic Identification

Chapter III – Trust Services

- Section 1 General provisions
- Section 2 Supervision
- Section 3 Qualified Trust Services
- Section 4 Electronic Signatures
- Section 5 Electronic Seals
- Section 6 Electronic time stamps
- Section 7 Electronic registered delivery services
- Section 8 Website authentication

Chapter IV – Electronic documents

Chapter V – Delegations of powers and implementing provisions

Chapter VI – Final provision

New structure

Chapter 1 – General provisions

Chapter II – Electronic Identification

Section I Electronic identification (European Digital Identity Wallet)

Section II Electronic Identification schemes

Section III Cross-border reliance on electronic identification means

Chapter III – Trust Services

- Section 1 General provisions
- Section 2 Supervision
- Section 3 Qualified Trust Services
- Section 4 Electronic Signatures
- Section 5 Electronic Seals
- Section 6 Electronic time stamps
- Section 7 Electronic registered delivery services
- Section 8 Website authentication
- Section 9 Electronic attestations of attributes
- Section 10 Qualified electronic archiving services
- Section 11 Electronic ledgers

Chapters IV, V, VI

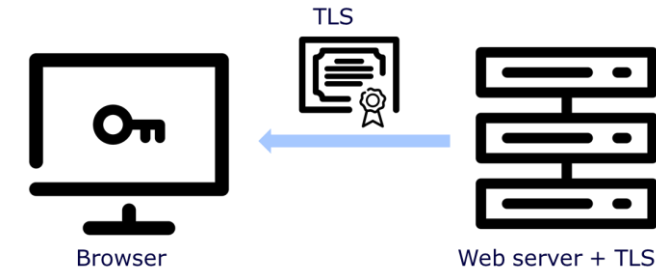
ANNEX V – Requirements for Electronic Attestations of Attributes

ANNEX VI – Minimum List of Attributes

Quelle: DG CNECT beim European Signature Dialog 21 Juni 2021

Was sind QWACs

- Ein eIDAS Vertrauensdienst
- klassische TLS Zertifikate gemäß RFC 5280
- Validierbar gegen die EU Trusted List
- Nach Erwägungsgrund 67 der eIDAS "Website-Authentifizierungsdienste geben dem Besucher einer Website die Sicherheit, dass hinter der Website eine echte und rechtmäßige Diese Dienste tragen zur Vertrauensbildung in der Abwicklung des elektronischen Geschäftsverkehrs bei, da die Nutzer einer authentifizierten Website vertrauen werden "
- QWAC wird im Einklang mit den Regeln der EU genutzt werden



Der Browser Vertrauensraum

- Vorgaben: Root Store Policy, Baseline Requirements, EV-Guidelines
- Technische Umsetzung: Root Store
- Verantwortlichkeit: Browser
- Überwachung: Qualifizierte Auditoren und CCADB

European Digital Single Market

- Vorgaben: EU-Verordnung eIDAS, referenzierte Durchführungsrechtsakte und technische Standards
- Technische Umsetzung: EU Trusted List und nationale eIDAS Trusted Lists
- Verantwortlichkeit: EU Kommission
- Überwachung: Supervisory Bodies und Konformitätsbewertungsstelle

Qualifizierter Vertrauensdienstanbieter (qVDA)

- Nutzer und Zertifikatsinhaber sollen das QWAC im Browser nutzen können
- Browser betreiben ihren eigenen Vertrauensraum
- Die EU behält ihre Souveränität über das QWAC

Aktueller Stand

- Es zeichnet sich eine Einigung im Trilog ab
- Artikel 45 in eIDAS bleibt erhalten.
- Die eIDAS Novellierung wird vermutlich Ende des Jahres veröffentlicht.
- qVDA, Browser und weitere Stakeholder überarbeiten bei ETSI die Standards
- Durchführungsrechtsakt wird für Ende 2024 erwartet

Die Konflikte bleiben, aber es zeichnen sich Lösungen ab

Gründe für QWACs

- Unterstützung der Ziele der DSGVO
 - Websites die nach persönlichen Daten fragen, sollen den verantwortlichen Data Controller anzeigen
Art 5 Abs 1 lit (f) DSGVO Integrität und Vertraulichkeit
 - QWAC liefern diese Information
- Unterstützung der Authentifizierung:
 - Verschlüsselung des Kommunikationskanals (Transportsicherung)
 - Offenlegung der Kommunikationspartner
 - Ein Beispiel ist die Authentifizierung in der Payment Services Directive (PSD2) -> RTS on SCA
- Mögliche Unterstützung der EUDI Wallet der eIDAS 2.0:
 - Verschlüsselung des Kommunikationskanals (Transportsicherung)
 - Offenlegung der Kommunikationspartner
 - Schutz vor Quishing oder QRL Jacking
 - Authentifizierung bei Authentic Sources (Artikel 45 d Allgemeine Ausrichtung der eIDAS 2.0)

QWAC seit 2018 erfolgreich im Finanzsektor (PSD2)

Widespread Use

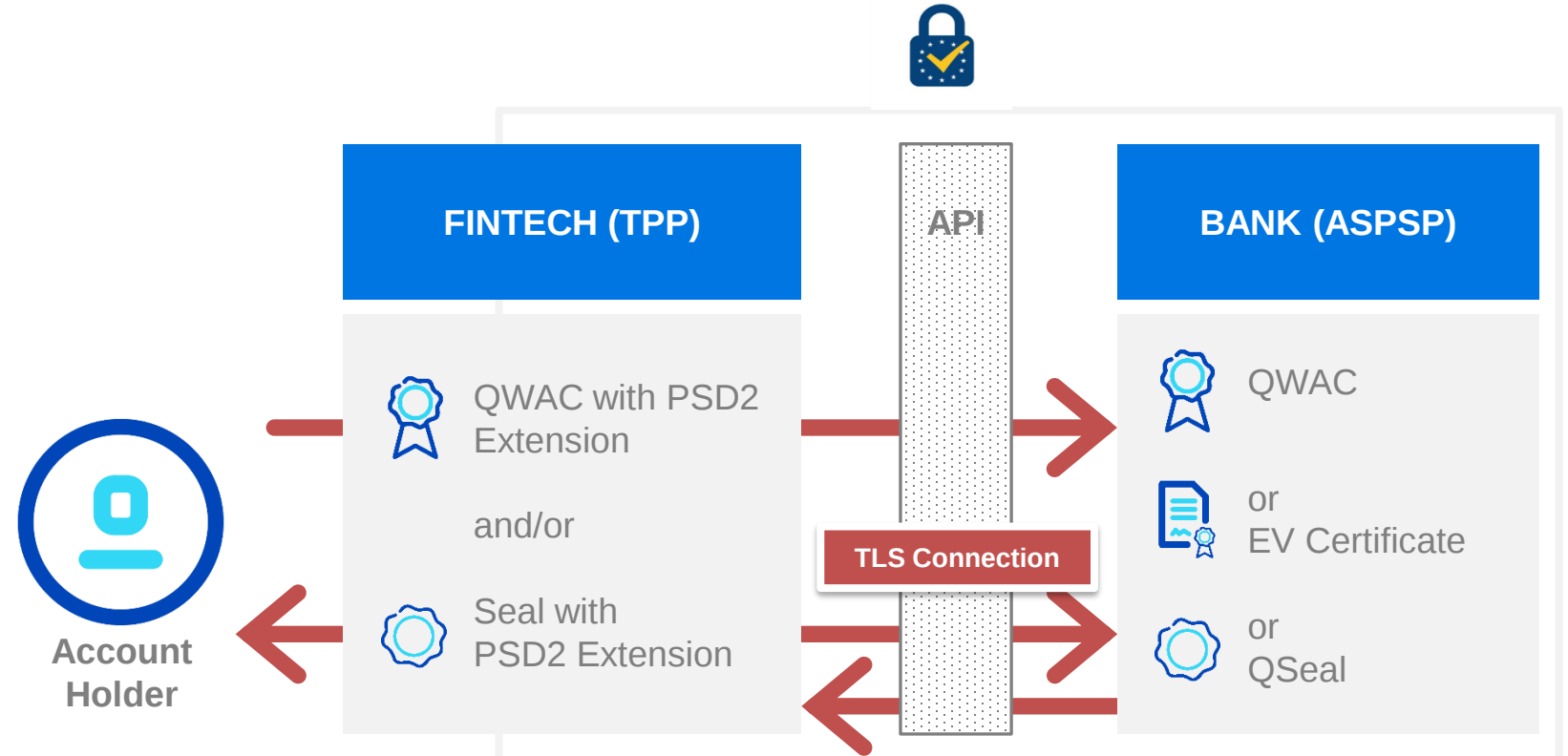
- Bank APIs live since 9/2019
- 400+ TPP and ~6000 Banks in the EU participating
- Special attributes in the certificate
- approx. 20 active QTSPs
- 9 Providers, 16 Brands

High throughput

- 530+ Mio. API calls p.m.
- Response time ~623ms, getting faster

Security and ease of use by eIDAS

- Connections are TLS secured and use eIDAS qualified seals and QWAC
- can be **easily validated** against the EU Trusted List*

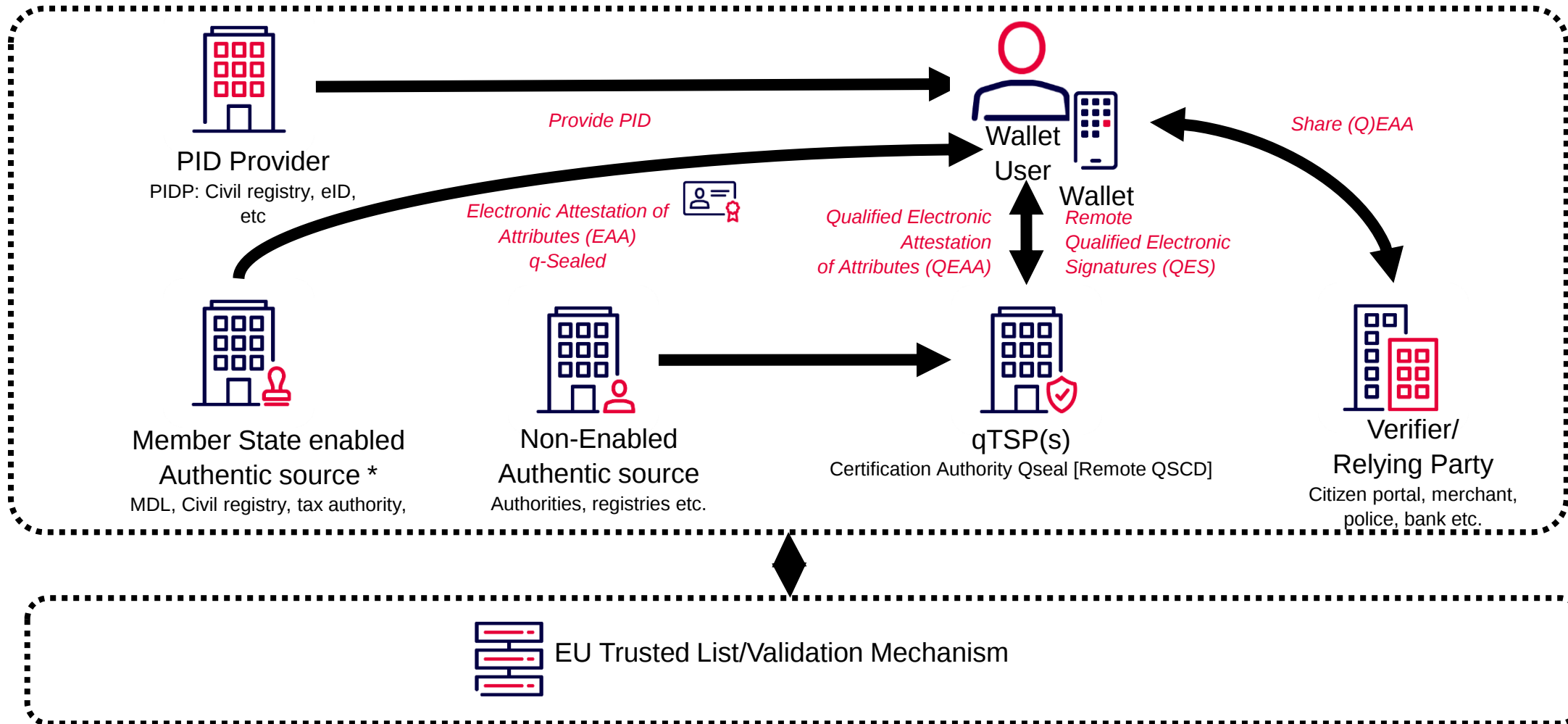


QWAC bei Registerauthentifizierung (authentic source)

Artikel 45 d der Allgemeine Ausrichtung der eIDAS 2.0

- Member States shall ensure within 24 months after entry into force of the implementing acts referred to in Article 6a(11) and Article 6c(4) that, at least for the attributes listed in Annex VI, wherever these **attributes rely on authentic sources within the public sector, measures are taken to allow qualified providers of electronic attestations of attributes to verify these attributes** by electronic means at the request of the user and in accordance with national or Union law.

EUDI Wallet Ökosystem

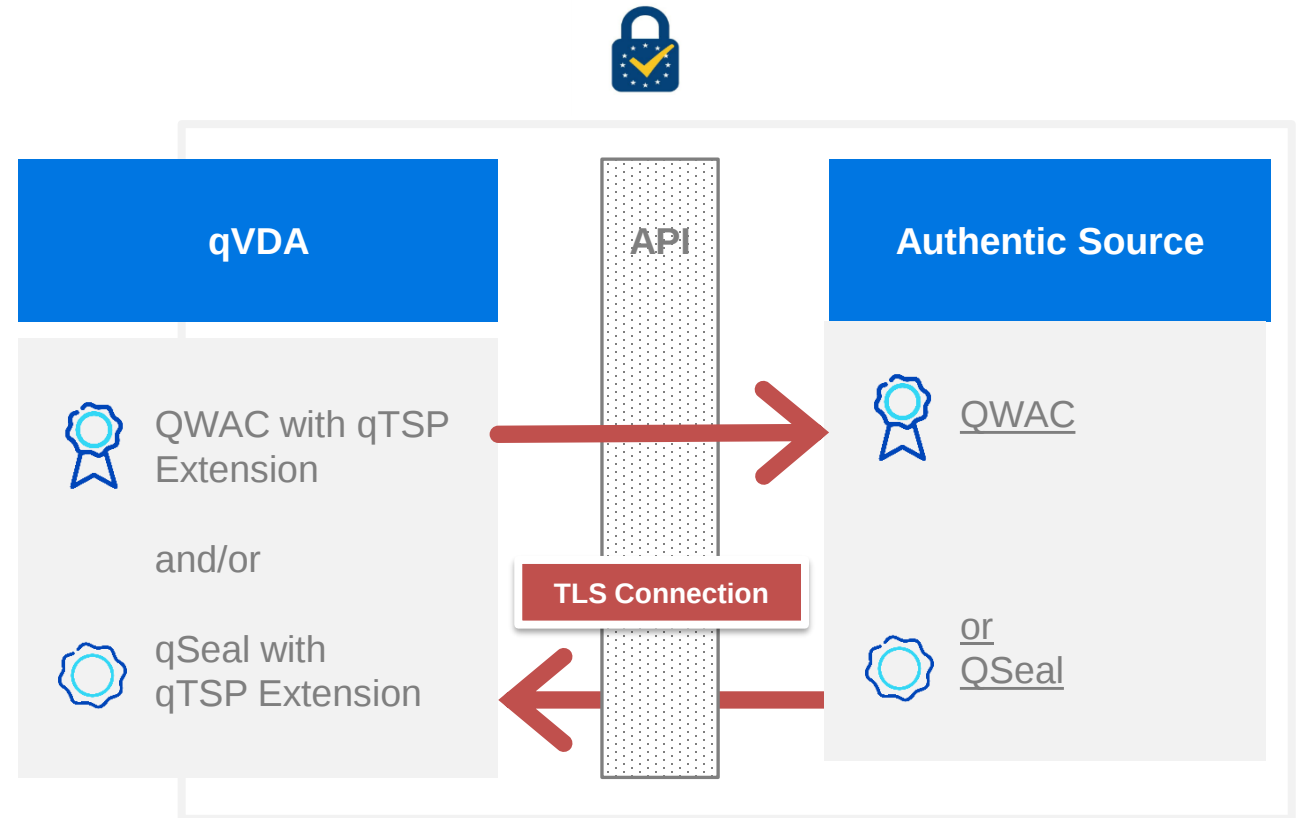


*Artikel 45d(a) & Artikel 3 (45a) des eIDAS-Proposals des Rates (Allgemeine Ausrichtung)

Vorschlag „PSD2 Modell“ für den Zugriff auf die Authentic Sources

- Nebenbedingung
Jede Authentic Source veröffentlicht seine API und den Zugriff darauf
- Vorteil
Es braucht kein Standard über alle Authentic Sources

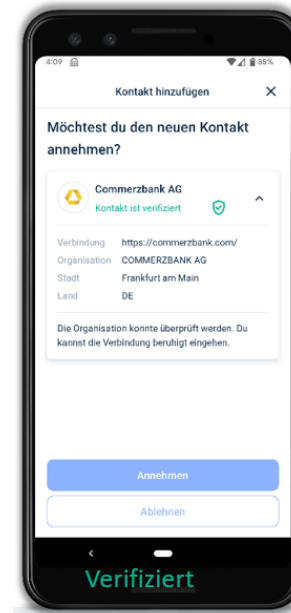
Jede Authentic Source kann unabhängig ihre Schnittstelle weiter entwickeln



Mögliche Verwendung von QWAC bei der EUDI Wallet

Mögliche Darstellung der Vertrauensbeziehung in der Wallt

DV	QWAC / EV	
09:25 Warning above keyboard is shown because user selected input field for no identity site Please sign in Email address Password ☐ Remember me Sign in Site owner unknown! Don't enter any personal data 1 2 3 4 5 6 7 8 9 0 q w e r t y u i o p	09:25 Identity summary above keyboard is shown because user selected input field for identity site Please sign in Email address Password ☐ Remember me Sign in Example B.V. Noord-Holland, NL Private organization (1234567890) 1 2 3 4 5 6 7 8 9 0 q w e r t y u i o p	09:25 Identity details above keyboard is shown because user clicked on summary Please sign in Email address Password ☐ Remember me Example B.V. Nieuwezijds Voorburgwal 147 1012 RJ Amsterdam Noord-Holland, NL Private organization (1234567890) 1 2 3 4 5 6 7 8 9 0 q w e r t y u i o p



Users receive context-based assistance and recommendations for action when identifying a requesting organization

Organizations that can prove their identity with the help of "QWAC" certificates receive a green tick.



- Requestors who cannot sufficiently prove their identity are marked with clear warnings
- First stage in the detection of phishing and MITM attacks
- More information at: <https://lissi-id.medium.com/vertrauen-im-digitalen-raum-cc22a9fcbd0a>